E-ISSN 2619-6301 No. 14, Año 2021

ANÁLISIS DEL *PHISHING* Y LA LEY DE DELITOS INFORMÁTICOS EN COLOMBIA

Jaiver Julián Medina Martínez*, Camilo Hernán Cárdenas Osorio**, Mauricio Mejía Lobo***

RESUMEN

Las tecnologías de la información siguen y seguirán evolucionando. Esta situación conlleva drásticos cambios en la sociedad y en el uso que se les den. Dentro de los usos, como toda herramienta, pueden estos tener sus bondades, así como sus efectos o usos negativos, los cuales son explotados por una minorías, pero con unos impactos drásticos y altos. Como respuesta a esto los gobiernos, desde sus poderes legislativo, ejecutivo y judicial, interponen leyes y grupos para el seguimiento y la judicialización de quienes las usan con fines delictivos. De allí nacen varias inquietudes, como, por ejemplo, la seguridad y el conocimiento, por lo cual se emprende una revisión bibliográfica centrada en el *phishing* con el fin de determinar el estado frente a este reconocido delito en aumento.

Palabras clave: *Phishing*, Delitos Informáticos, Suplantación, Robo De Identidad, Ciberseguridad

* Correo electrónico: jaiver.medinama@amigo.edu.co
** Correo electrónico: camilo.cardenasos@amigo.edu.co
*** Correo electrónico: mauricio.mejialo@amigo.edu.co

INTRODUCCIÓN

El concepto de *phishing* se puede definir como un método usado para sustraer información y obtener beneficios económicos a partir de ello.

Según el gremio representativo del sector financiero colombiano Asobancaria (2019), el *phishing* es una modalidad de fraude que consiste en el envío masivo de mensajes electrónicos en los que aparece una dirección web falsa o clonada de una entidad bancaria, con el fin de capturar información sensible de los usuarios, como, por ejemplo, sus claves de acceso, etc.

La palabra *phishing* proviene de la analogía que los primeros criminales de internet establecieron al usar señuelos de correo electrónico para *phish* ("pesca") de contraseñas y datos financieros de un mar de internautas. El uso del "ph" en la terminología se pierde con el tiempo, pero lo más probable es que esté vinculado a convenciones populares de nombres de *hackers* tales como "phreaks", que se remonta a los hackers tempranos que estaban involucrados en "phreaking" —el *hacking*— de los sistemas de telefonía (Ollmann, 2017).

Phishing es un delito informático que se rastrea hace más de veinte años. Por supuesto, en esa época no tenía tal nombre, si bien para 1990 ya existían personas maliciosas y delincuentes que enviaban correos electrónicos solicitando información personal. Según el artículo de Matute (2013), el término se conoce seis años más tarde del primer ataque dirigido a la empresa estadunidense America On Line.

La primera mención del término *phishing* fue en enero de 1996. Se dio en el grupo de noticias de *hackers* alt.2600, aunque es posible que ya hubiera aparecido aen la edición impresa del boletín de noticias *hacker 2600 Magazine*. El término *phishing* fue asignado para quienes pretendían apoderarse de cuentas de miembros de AOL.

La historia señala que los primeros casos de *phishing* se detectaron a mediados del 1990 por la empresa estadounidense America On Line. El estafador enviaba un correo electrónico solicitando diversa información de facturación, entre las que se encontraban los números de las tarjetas de crédito empleadas para pagar por el servicio (Ayala, 2011).

Método

Se trata de una revisión teórica mediante una búsqueda exhaustiva del material en la que se logró identificar quince documentos, de los cuales se hizo la abstracción sobre los resultados más significativos y se presenta el resultado.

Tipos de *phishing*

Los tipos de *phishing* se enlistan y describen a continuación.

- *Spear phishing.* Está dirigido a personas específicas o a grupos reducidos. De esta manera, las campañas son mucho más personalizadas y dirigidas, de modo que aumenta el número de víctimas. Según Kaspersky (2019b), el funcionamiento del *spear phishing* es el siguiente: llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a

E-ISSN 2619-6301 No. 14, Año 2021

un sitio web falso con gran cantidad de *malware*. Estos correos utilizan técnicas inteligentes para captar la atención de las posibles víctimas.

- *Whale phishing/whaling*. Esta clase de *phishing* tiene como objetivo funcionarios gerenciales de las empresas. Al igual que en el *spear phishing*, se realiza un estudio previo de la posible víctima personalizando el mensaje para que sea más efectivo. La empresa estadounidense desarrolladora de antivirus Trend Micro (2018) plantea en su página web oficial lo siguiente sobre el *phishing* ballena): El *phishing* de ballena es un término usado para describir un ataque de *phishing* dirigido específicamente a personas adineradas, poderosas o prominentes. Debido a su estado, si un usuario de este tipo se convierte en víctima de un ataque de *phishing* puede ser considerado un "gran phish" o, alternativamente, una "ballena".
- *Social phish*. Es un modelo dentro de la terminología *phishing* que hace énfasis en herramientas web para la clonación de alguna red social, ya sea Facebook, Twitter, LinkedIn, etc., ya que cuenta con algunas "plantillas" y a la vez bajo segundo nivel de desarrollo abstrae y copia la información personal de los usuarios en una base de datos.
- *Shellphish*. Provee una interfaz de usuario para acceder a los servicios del sistema operativo del equipo infectado con el malware.

Ahora bien, el *pharming* es una combinación de los términos *phishing* y *farming*. El *pharming* aprovecha los principios con los que funciona la navegación por internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de internet, como, por ejemplo, www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión. El *exploit* ataca este proceso de dos maneras. En primer lugar, un *hacker* puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de *hosts* de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso. En segundo lugar, el *hacker* puede infectar un servidor para que los usuarios visiten el sitio falso sin darse cuenta.

Cifras internacionales

Según la fuente BITTIN SAS, para el 2018 el cibercrimen dejó ganancias por encima de los tres trillones de dólares, lo que representó para América Latina USD 6179 millones. Para el 2020, de acuerdo con las estimaciones y proyecciones y según el efecto de la cuarentena mundial, se ha presentado un aumento considerable tasado en más del 30 % de las ocurrencias, con un especial énfasis en el *phishing*.

El mundo digital se ha integrado a toda la sociedad de una forma vertiginosa. En nuestro diario vivir son más las personas que se apoyan en internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre IP, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas (Clavijo, 2006).

Cifras en Colombia

Según Clavijo (2006), para Colombia el negocio de los ciberdelitos dejó 31.498 denuncias. Los tipos de industrias más afectadas fueron el financiero con un 40 %, el de telecomunicaciones con un 26 %, el gubernamental con un 16 %, el de productos con un 10 % y el energético con una tasa del 9 %.

A su vez, según los tipos de delitos cibernéticos, el *phishing* se encuentra en el primer lugar en el país, seguido de la *sextorsión*, el *vishing*, *SIM swapping*, el *formjacking* y el secuestro de información. Según el Centro Cibernético Policial, durante el 2017 se evidenció un aumento significativo en conductas delictivas que vulneran la integridad de las personas. El "Artículo 269I. Hurto por medios informáticos y semejantes" es la tipología criminal de mayor frecuencia, equivalente al 60 %, seguido del "Artículo 269F. Violación de datos personales", con el 16 %, y del "Artículo 269A. Acceso abusivo a un sistema informático". (Centro Cibernético Policial, 2017).

Legislación internacional

Naciones Unidas, Asamblea General, documento A/74/130: Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, Informe del Secretario General

El informe se ha preparado en cumplimiento de la Resolución 73/187 de la Asamblea General, titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos". En esa resolución, la Asamblea General solicitó al Secretario General que recabara las opiniones de los Estados miembros sobre los problemas a los que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, y que presentara un informe basado en esas opiniones a fin de examinarlo en su septuagésimo cuarto periodo de sesiones. Contiene información de los Estados miembros presentada en cumplimiento de la resolución.

Convención de Budapest

El 23 de noviembre del 2001 tuvo lugar en Budapest, Hungría, un consejo de ministros de Europa, denominado "Convenio sobre la ciberdelincuencia". En este se establecen cuáles son en su momento las conductas delictivas de los ciberdelincuentes y las leyes para afrontarlas (Consejo de Europa, 2001).

Legislación en Colombia

La Ley 1273 de 2009, "De la protección de la información y de los datos", en su articulado señala los siguiente:

> Artículo 269G*: Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma

E-ISSN 2619-6301 No. 14, Año 2021

> sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Cabe aclarar que, aunque literalmente los términos *phishing* e *ingeniería social* no están contemplados en los artículos del Código Penal del 2009, sus acciones delictivas son las que irrumpan frente a la ley y ocasionen sanciones según su estado de acción.

Ley 1298 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Conclusiones

La seguridad de la información es de gran importancia y debe ser un tema estratégico y crítico. Por tal motivo, debe ser prioridad estar actualizados en las nuevas formas de seguridad de la información organizacional y la evolución de los *malware*, para así estar en capacidad de tomar las medidas más adecuadas con miras a contrarrestar estos ataques.

Se debe estar actualizado en delitos informáticos, ya que nos ayudará a tener más cuidado con las páginas a las que se ingresa y no brindar nuestra información personal, a fin de evitar que nos ataquen el cibercrimen.

Agradecimientos

A la Universidad Católica Luis Amigó.

REFERENCIAS

AO Kaspersky Lab. (2019a). Ingeniería social: definición. Kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

AO Kaspersky Lab. (2019b). ¿Qué es el spear *phishing*? Kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/spear-*phishing*

Asobancaria. (2019). Saber más ser más. Programa de educación financiera de los bancos en Colombia. Phishing. Asobancaria.com. http://www.asobancaria.com/sabermassermas/*phishing*/

Bittin. Investigación digital, Informática forense, Recuperación y confidencialidad de la información. Bittin.co. www.bittin.co

Centro Cibernético Policial. (2017, diciembre). Balance Cibercrimen en Colombia 2017. https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Clavijo, C. A. (2006, enero-julio). Políticas de seguridad informática. *Entremados, 2*(1), 86-92. http://www.redalyc.org/articulo.oa?id=265420388008

Congreso de la República de Colombia. (2009, enero 5). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. DO 47.223.

Congreso de la República de Colombia. (2018, julio 24). Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. DO 50.664.

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia*. Consejo de Europa.

Matute, J. C. (2013). El delito informático de *phishing*. http://dspace.uniandes.edu.ec/handle/123456789/2819

Oxman, N. (2013, noviembre, 13). Estafas informáticas a través de Internet: acerca de la imputación penal del "*phishing*" y el "pharming". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 41. https://scielo.conicyt.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext&tlng=en

Ollmann, G. (2017). *The Phishing Guide*. Estados Unidos de América. http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf

Pérez, Y. (2017). Un caso de phishing más en Colombia. Universidad Cooperativa de Colombia. Ucc.edu.co. Recuperado de https://www.ucc.edu.co/noticias/conocimiento/ingenieria-arquitectura-y-urbanistica/un-caso-de-phishing-mas-en-colombia